UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,786	06/23/2006	Mounir Kellil	CML01203EP	1460

22917 7590 04/02/2009

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	10/596,786	KELLIL ET AL.	
	Examiner	Art Unit	
	CARL COLIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 December 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 12/23/2008, Applicant amends claims 1, 3, 6, and 9. The following claims 1-10 are presented for examination.

1.1 In response to communications filed on 12/23/2008, the objection to the specification and to the drawings has been withdrawn with respect to the amendment.

1.2 Applicant's arguments filed on 12/23/2008 have been fully considered but they are not persuasive. Regarding the 112th rejection first paragraph Applicant amends the claims to change visiting group member to mobile member. However, the original specification as filed still does not provide enough support for both conditions to be true to sending a new visitor encryption key as claimed.

The claim recites: "*sending a new Visitor Encryption Key (VEK.sub.j) to a mobile member (MMj.sub.j) arriving in the corresponding group key management area (area.sub.j) if there is no other mobile member (MMl.sub.j) situated in the corresponding group key management area (area.sub.j) and if a current Visitor Encryption Key (VEK.sub.j) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK).*"

The specification page 13, lines 1-16 discloses

"- if there are no VEKj members the CGKS generates and sends a VEKj key,

- **if there are VEKj members and the current key was used to encrypt the previous (TEK), provide a new key VEKj** to the entering mobile member".

Therefore, the claims are still rejected under 35 USC 112th rejection first paragraph.

Regarding the prior art rejection, Applicant generally alleges (see pages 10-11) that Hardjono does not disclose extra key owner lists that distinguish between group members of different areas. Examiner respectfully disagrees as Hardjono discloses storing domain keys for different domains. In addition, Applicant does not provide any explanation that shows an error in Examiner's rejection. Applicant also argues *"Applicant's visiting member is a group member that is visiting a group key management area within a multicast group. In contrast, Hardjono's client is not a group member visiting from one area to another within the multicast group"*. Examiner respectfully disagrees as the claim does not recite such features. Applicant further argues about the claim as amended recites: "*sending a new Visitor Encryption Key (VEK.sub.j) to a mobile member (MMj.sub.j) arriving in the corresponding group key management area (area.sub.j) if there is no other mobile member (MMl.sub.j) situated in the corresponding group key management area (area.sub.j) and if a current Visitor Encryption Key (VEK.sub.j) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK).*" However, as shown above, these claim limitations are not supported by the original specification.

Upon further consideration, Applicant has not overcome the prior art and the claims remain rejected.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 1 recites : "*sending a new Visitor Encryption Key (VEK.sub.j) to a mobile member (MMj.sub.j) arriving in the corresponding group key management area (area.sub.j) if there is no other mobile member (MMl.sub.j) situated in the corresponding group key management area (area.sub.j) and if a current Visitor Encryption Key (VEK.sub.j) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK).*" The original specification does not describe a situation for a new Visitor Encryption Key (VEK.sub.j) to a mobile member (MMj.sub.j) arriving in the corresponding group key management area (area.sub.j) where both conditions are mentioned as claimed such as no other mobile member and a current VEKj was already used to encrypt a previous TEK (see specification, page 13, lines 1-16).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,584,566 to **Hardjono** *(Applicant's IDS)*.

As per claim 1, **Hardjono** discloses a method of inter-area rekeying of encryption keys in secure mobile multicast communications, comprising *distributing Traffic Encryption Keys (TEK) to a plurality of local Group Controller Key Servers (local GCKS) serving respective group key management areas,*(see column 4, lines 30-53 and lines 63-64, distributing group related keys to key servers) *and said local Group Controller Key Servers forward said Traffic Encryption Keys, encrypted using Key Encryption Keys (KEK.sub.i, KEK.sub.j) that are specific to the respective local Group Controller Key Server (local GCKSi, GCKS.sub.j), to group members situated in the respective group key management areas,*(see column 5, lines 15-35 and line 55 through column 6, line 3 disclosing forwarding keys to respective members) (see column 7, lines 39-45 disclosing keys are encrypted using specific key encryption keys belonging to the

particular groups) *said local Group Controller Key Servers (GCKSj, GCKS.sub.j) constituting Extra Key Owner Lists (EKOLj, EKOL.sub.j) for said group key management areas (areaj, area.sub.j) that distinguish group members (MMi, MM.sub.j) possessing Key Encryption Keys (KEKj, KEKj) and situated in the corresponding group key management area (areas, area.sub.j) from group members (MMy) possessing Key Encryption Keys (KEKj) that were situated in the corresponding group key management area (areaj) but are visiting another area (area.sub.]),* (see column 9, lines 39-45); *forwarding said Traffic Encryption Keys (TEK) to group members (MMj.sub.j) visiting the respective group key management areas (area.sub.j) encrypted using a Visitor Encryption Key (VEK.sub.j) that is specific to the respective local Group Controller Key Server (GCKS.sub.j) and is different from said Key Encryption Key (KEK.sub.j)* (see column 10, lines 27-35 disclosing using a member key to encrypt members joining the group key management area) *and sending a new Visitor Encryption Key (VEK.sub.j) to a mobile member (MMj.sub.j) arriving in the corresponding group key management area (arca.sub.j) if there is no other mobile member (MMl.sub.j) situated in the corresponding group key management area (area.sub.j) and if a current Visitor Encryption Key (VEK.sub.j) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)* (see column 10, lines 27-35 disclosing sending new key to the member M10 joining and there is no mention of other visiting members).

As per claim 2, **Hardjono** discloses rekeying said Traffic Encryption Keys (TEK) after rekeying said Key Encryption Key (KEK.sub.i, KEK.sub.j). (see column 9, lines 1-5 and 23-25 disclosing new domain key after replacing common key).

As per claim 3, **Hardjono** discloses rekey a Key Encryption Key (KEK,, KEK,) by a process comprising sending new Key Encryption Key (KEK, KEK.) to current group members encrypted using the current Key Encryption Key (KEK,KEK,) and to mobile members using the Visitor Encryption Key (VEK,VEK,) (see column 10, lines 5-35).

As per claim 4, **Hardjono** discloses wherein said local Group Controller Key Server GCKS, sends the Visitor Encryption Key (VEK,) rather than the Key Encryption Key (KEK,) to new members joining the group via area, (see column 10, lines 5-35, disclosing distributing the member key rather than the current domain key).

As per claim 5, **Hardjono** discloses wherein said local Group Controller Key Servers (GCKS,, GCKS,] rekey a Key Encryption Key (KEK,, KEK,) by a process comprising sending said new Key Encryption Key (KEK,, KEK,) selectively to existing group members situated in the corresponding group key management area (see column 10, lines 1-35).

As per claim 6, **Hardjono** discloses wherein said local Group Controller Key Servers (GCKS,, GCKS,) rekey a Key Encryption Key (KEK,, KEK,) by a process comprising sending said new Key Encryption Key (KEK,, KEK,) to existing group members using multicast messages and to mobile members over a different secure channel (see column 10, lines 1-35).

As per claim 7, **Hardjono** discloses wherein rekeying a Key Encryption Key (KEK,, KEK,) comprises said local Group Controller Key Servers (GCKS,, GCKS,) by a process

comprising sending a new Key Encryption Key (KEK,, KEK,) selectively to current group members currently situated in the corresponding group key management area (see column 10, lines 1-35).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,584,566 to **Hardjono** *(Applicant's IDS)* in view of Non Patent Literature "Secure Group Communications for Wireless Networks" pages 113-117 by **Decleene et al**.

As per claim 8, **Hardjono** discloses the claimed method of claim 3 but is silent about disclose distinguish group members (MMi, MMj) possessing Visitor Encryption Keys (VEKi, VEKj) and situated in the corresponding group key management area (areai, areaj,) from group members possessing Visitor Encryption Keys (VEKi) that were situated in the corresponding group key management area (areai) but are visiting another area (areaj). **DeCleene et al** in an analogous art discloses distinguishing members within an existing area and member possessing key that were situated in the corresponding area but are visiting another area wherein the members may be excluded during updating (see pages 114-115). Therefore it would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify **Hardjono et al** to have a list of current members and members visiting so that different keys are distributed to them respectively as suggested by **DeCleene et al** (see pages 114-115).

As per claim 9, the references as combined above disclose wherein said Extra Key Owner Lists (EKOL, EKOLj) and said Visitor Key Qwner Lists (VKOL,, VKOLj) comprise lists of the group members (MM,) possessing Key Encryption Keys (KEK,), Visitor Encryption Keys (VEK,, VEK,), respectively that were situated in the corresponding group key management area (area,) but are visiting another area (area,) (see **DeCleene et al,** pages 114-115). Claim 9 is also rejected on the same rationale as the rejection of claim 8.

As per claim 10, the references as combined above disclose wherein a group member that was visiting another group key management area (area,) returns to an area (area,) for which it possesses a corresponding Key Encryption Key (KEK,) or Visitor Encryption Key (VEK,) before expiry of a validity period set by the corresponding Group Controller Key Server (GCKS,) without said corresponding Croup Controller Key Server (GCKS,) rekeying said Key Encryption Key (KEK,) (see **DeCleene et al,** pages 114-115). Claim 10 is also rejected on the same rationale as the rejection of claim 8.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2436
March 27, 2009